

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.  | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO.  | CONFIRMATION NO. |
|--|-------------|----------------------|----------------------|------------------|
| 09/652,157   | 08/31/2000  | Motoji Oomori        | 04329.2371           | 2617             |
| 22852  | 7590        | 08/24/2004           | EXAMINER             |                  |
| FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER<br>LLP<br>1300 I STREET, NW<br>WASHINGTON, DC 20005 |             |                      | SIMITOSKI, MICHAEL J |                  |
|  |             |                      | ART UNIT             | PAPER NUMBER     |
|  |             |                      | 2134                 |                  |

DATE MAILED: 08/24/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

**Application No.**

09/652,157

**Applicant(s)**OOMORI ET AL. **Examiner**

Michael J Simitoski

**Art Unit**

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
  - If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
  - If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
  - Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 08 June 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 27-46 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 27-30, 33-39 and 42-46 is/are rejected.
- 7) ☒ Claim(s) 31, 32, 40 and 41 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 31 August 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some \* c) ☐ None of:
- 1) ☒ Certified copies of the priority documents have been received.
  - 2) ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - 3) ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 6/25/04.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

**DETAILED ACTION**

1. The response of 6/14/2004 has been received and considered.
2. Claims 27-46 are pending.

***Claim Rejections - 35 USC § 102***

3. Claims 27, 28, 30, 35-37 & 39 are rejected under 35 U.S.C. 102(b) as being anticipated by Miyano.

***Claim Rejections - 35 USC § 103***

4. Claims 29 & 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano.
5. Claims 33, 42 & 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano, as applied to claims 28 & 36, in view of U.S. Patent 5,787,179 to Ogawa.
6. Claims 44 & 45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano in view of Srinivasan.
7. Claims 34 & 43 are rejected under 35 U.S.C. 103(a) as being unpatentable over Miyano, as applied to claims 33 & 42, in view of Schneier.
8. For further details of the above rejections, see the Office Action dated 3/8/2004.

***Response to Arguments***

9. Regarding claims 27-28, 30, 33, 35-37, 39 & 42, applicant's arguments of 6/14/2004 (pp. 2-4) have been considered, but are not persuasive. The Office Action dated 3/8/2004 details how

Art Unit: 2134

the Miyano reference teaches the following limitations of independent claims 27, 35, 36 & 37:

“a nonlinear transform unit ...”, “an expansion unit ...” and “an expansion key calculation unit ...”, whose existence is argued by applicant.

10. Regarding claims 29 & 38, the Examiner cites U.S. Patent 6,256,391 to Ishiguro et al. (Fig. 21 & col. 17, lines 10-21), U.S. Patent 5,703,952 to Taylor (col. 11, lines 41-50), U.S. Patent 4,255,811 to Adler (claims 5 & 11) and in particular, U.S. Patent 4,802,217 to Michener (col. 11, line 15 – col. 13, line 63) as references corroborating the prevalent use of a shift amount relatively prime to the number of output bits.

11. Regarding claims 32 & 41, upon further review of the claims and the prior art the Examiner withdraws the rejections made based on Official Notice.

12. Regarding claim 46, applicant's arguments (p. 6) have been considered but are not persuasive. Ogawa teaches a well-known concept where random number generators are used in encryption circuits to generate random numbers using a key as a seed input (col. 6, lines 20-31). The limitation that Ogawa teaches is merely an application or use of a key. Therefore, the rejection is maintained.

13. Regarding claims 44 & 45, applicant's arguments (p. 7) have been considered but are not persuasive. The Miyano teaches a method and basic functional components, but lacks a concrete, physical implementation (as many variations are possible). Srinivasan is relied upon for teaching a well-known concept in computer architecture, whereby taking steps to be performed and performing them on parallel hardware increases the speed and throughput of a calculation circuit. While Miyano does not disclose a register for the constants applied, it is inherent that the inputs and values used in Miyano's calculations must be held in some storage

element before being accessed by a circuit/functional unit. Therefore, the rejection is maintained.

14. Regarding claims 34 & 43, applicant's arguments (pp. 7-8), Miyano does not disclose common substitution elements. Miyano's device performs the same basic cryptographic function as FEAL (disclosed in Schneier), which is a variant of DES. Miyano further briefly describes DES (col. 1, lines 32-56) and how it has been improved upon. The substitution elements used are widely known to be a part of block ciphering algorithms, as taught by Schneier's Applied Cryptography, Second Edition which is a book on general concepts in the field of cryptography. Therefore, the rejection is maintained.

#### ***Allowable Subject Matter***

15. Claims 31-32 & 40-41 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

#### ***Conclusion***

16. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

17. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. - 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

**Any response to this action should be mailed to:**

Commissioner of Patents and Trademarks  
Washington, DC 20231

**Or faxed to:**

(703)746-7239 (for formal communications intended for entry)

**Or:**

(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



MJS  
August 16, 2004



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100